

Certified Security Compliance Specialist™ (CSCS™) A 2-Day Instructor-Led Security Compliance Program



Program Testimonials

“The training was comprehensive in covering the major legislations affecting several industries. Real world experiences was beneficial and relevant.”

Christine Kinyenje, CISSP
Lockheed Martin

“This was an excellent class. Finally, a program that encompasses all regulations an organization needs to be aware of and consider when conducting their business.”

Jeff Bontsas
Ascension Health

“The CSCS class provided a great overview of the requirements and definitions for many regulatory requirements. It is a must-do for every security professional to use as reference as their business/agencies grow.”

Kari Garland
Riverside County, California

“Pabrai is well versed in a multitude of laws, regulations and standards. If your organization must comply with information security requirements, you will do well to take the CSCS course.”

Tony Lewis
Intuit, Inc.

“Extremely comprehensive program giving one the advantage point of understanding security from all unified industries and then to be able to apply it to others. Program is thought provoking. Enable the participant to take the concept and think of areas that they need to focus on to make their environment/organizations better.”

Brian Lane, Vice President
American Hospital Association (AHA) Solutions

Why CSCS?

Increasingly, businesses are challenged with both securing their digital assets and the information infrastructure as well as achieving full compliance with legislations that impact their industry. Healthcare, financial, government and other verticals are required to constantly monitor the changing dynamics of their infrastructure to mitigate risks and vulnerabilities as well as ensure compliance with international as well as U.S. federal and state legislations and industry best practices. Further, United States federal information systems and those of their business associates must meet specific certification and accreditation security guidelines.

CSCS™ Program Covers Major Information Security Regulations & Standards

The CSCS™ Program is the first and only program in the world that provides a comprehensive treatment of major information security regulations and standards. You can expect to learn and understand core requirements of the following from the CSCS™ program:

- ISO 27002 (ISO 17799:2005)
- PCI DSS
- Sarbanes-Oxley Section 404 – Information Security Requirements
- FISMA
- HIPAA

The Certified Security Compliance Specialist™ (CSCS™) credential is a *job-role based designation*. This program is designed to enable professionals to understand, prioritize and ultimately assist organizations achieve compliance with information security-based regulations.

Compliance is big business. Legislations such as Sarbanes-Oxley, PIPEDA, FFIEC, HIPAA and standards such as the ISO 27002 (17799:2005) are a requirement for organizations to comply with. A key objective for organizations worldwide is to integrate security best practices and be in compliance. Skilled professionals who understand regulatory compliance requirements and information security are valued across several industries, especially healthcare, financial and the government.

The Certified Security Compliance Specialist™ (CSCS™) is a unique program of its type in the compliance and security industries - indeed the first of its type in the world. It is laser-beam focused on thoroughly examining compliance requirements and establishing best practices that can be applied in securing today's digital business information infrastructure.

Organizations are fast moving to a digital ecosystem that is governed by strict regulatory compliance requirements. Validate your compliance security skills and knowledge and distinguish yourself with the credential, Certified Security Compliance Specialist™ (CSCS™).

Distinguish Yourself in the Marketplace – Get the CSCS™ Credential!

Just having a background in Information Technology (IT) or information security is not sufficient anymore for the challenges of business today. Employers are looking for individuals who not only have IT skills but also understand compliance regulations that impact their industry and business – because these are priorities that must be met.

Certified Security Compliance Specialist™

- Validate your compliance security skills and knowledge. Distinguish yourself with the credential, Certified Security Compliance Specialist™ (CSCS™). Exam is conducted in the class towards the end of the 2nd day of the CSCS™ program.
- Prepare for the Certified Security Compliance Specialist™ (CSCS™) exam with the practice exam available exclusively for your convenience at www.ExamsOnline.com.
- All candidates that successfully pass the CSCS™ exam will receive a free set of information security policy template documents¹. Review sample enterprise security policies in class.

1. Is a one-user license and may only be used by CSCS™ candidate for 1 site at no additional cost. May not be distributed or copied without written authorization from ecfirst.com.

Learning Objectives

From this compliance and security training program you will:

- Examine the security aspects of the Sarbanes-Oxley (SOX) legislation with emphasis on key sections and critical compliance steps. Examine the COBIT security baseline.
- Learn about the Federal Information Security Management Act (FISMA), North American Electric Reliability Council (NERC) Cyber Security Standards, and the HIPAA Security Rule.
- Step through the core requirements of the Payment Card Industry (PCI) Data Security Standard (DSS).
- Analyze the international security standard, ISO's 27002 (17799:2005).
- Learn about authentication requirements for Internet Banking Environment - (FFIEC) guidelines.
- Examine California's SB 1386, AB 1950 and the GLBA legislation requirements
- Understand the security certification and accreditation process for U.S. federal information systems. This is an important requirement for business associates worldwide.
- Review international regulations including Canada's PIPEDA, Japan's PIP, European Union's DPD and EC Directive, Australia's Privacy Act, and the UK's Data Protection Act, Freedom of Information Act.
- Step through processes for conducting a comprehensive risk analysis and vulnerability assessments.
- Review key contingency compliance requirements for developing the framework for disaster recovery and emergency mode operation plans.

Prerequisite Requirements

- To be certified as a CSCS™, the candidate must attend the two-day CSCS™ training session delivered by the ecfirst.com Academy or any of its Authorized Partners. For a list of scheduled dates and locations, please visit www.ecfirst.com/Academy.
- It is strongly recommended that the candidate pass a major security certification exam such as CISSP, CISA or CISM or have equivalent knowledge and experience.

Target Audience

The complete two-day CSCS™ program is of value to compliance professionals and managers, security officers, security practitioners, privacy officers and senior IT professionals.

CISSPs

As (ISC)² CISSPs participate in this two-day instructor-led program and pass the CSCS™ exam, they are then responsible to document their time at [Continuing Professional Education \(CPE\)](https://www.isc2.org/cgi-bin/content.cgi?category=24), i.e. <https://www.isc2.org/cgi-bin/content.cgi?category=24> for possible eligibility for additional CPEs. The CSCS™ program offers 16 CPEs for CISSPs.

The CSCS™ Exam

The Certified Security Compliance Specialist™ (CSCS™) exam validates knowledge and skill sets in information security for the following legislations, standards and frameworks:

1. Financial Regulations (including PCI DSS, FFIEC, COBIT) & Security (20% of exam)
2. Digital Healthcare & Security (20% of exam)
3. ISO 27002 (17799:2005) and International Regulations (20% of exam)
4. Security Certification & Accreditation, FISMA (20% of exam)
5. Business Continuity Planning - (20% of exam)

Exam Name	Exam Number	Number of Questions	Time Allowed	Passing Score
CSCS-1	CSC-101	60	60 Minutes	75%

The first four sections of the CSCS™ exam focus in the area of “security” for regulatory compliance. The last section of the exam emphasizes the “availability” principle that is required by legislations.

CSCS™ exam questions are developed with the intent of measuring and testing practical knowledge and application of general concepts and standards in the area of *regulatory compliance and information security*. All questions are multiple choice and are designed with one BEST answer.

Every CSCS™ exam question has a stem (question) and five options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario or description problem may be included. These questions normally include a description of a situation and require the candidate to answer one or more questions based on the information provided.

The candidate is cautioned to READ the question carefully. Many times a CSCS™ exam question will require the candidate to choose the appropriate answer that is MOST LIKELY or BEST. In each instance, the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible.

All questions should be answered. There are no penalties for incorrect answers. Grades are based solely on the number of questions answered correctly; so do not leave any questions blank.

At the conclusion of each exam, test questions are reviewed. Questions identified as being ambiguous or having technical flaws will either not be used in the grading process or will be given multiple correct answer keys.

Course Outline

Module 1: Regulatory Compliance and Security

- Core Objectives
- U.S. Legislations
 - California's Privacy and Security Requirements
 - FDA's CFR 21
 - GLB
 - NERC CSS
- Important International Regulations
 - Japan's PIP
 - Canada's PIPEDA
 - Australia's Privacy Act
 - European Union's DPD
 - EC Directive
 - UK's Data Protection Act
 - UK's Freedom of Information Act

Module 2: Financial Services and Security

- Sarbanes-Oxley Section 404 Fundamentals
- Key Sections
- Technology and Security Impact
 - Security Architecture and Infrastructure
- CobiT Security Baseline
 - Control Objectives
 - Security Domains

Case Study: Examine FFIEC Guidelines for Internet Banking

Step through key requirements of U.S. federal government mandates for strong authentication that impacts banks offering online banking. Understand why in today's online financial services environment, authentication is the bedrock of information security.

Learn about the FFIEC guidance and how banks and financial institutions must balance risk, cost and customer experience when choosing authentication solutions.

Module 3: Digital Healthcare & Security

- Healthcare Security Challenges
- U.S. HIPAA Security Legislation
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Security Policies

Module 4: Payment Card Industry (PCI) Data Security Standard (DSS)

- Objective
- Control Objectives
- Defined Requirements
- Critical References

Module 5: ISO 17799:2005 Standard

- Objective
- Scope
- Key Domains
 - Definition
 - Requirements

Module 6: Security Certification and Accreditation

- U.S. Federal System Requirements
- Critical Processes & Phases
- Common Security Controls
- FISMA
 - Core Objectives & Requirements
 - Federal Information Security Incident Center
- Key U.S. Government Security References & Guidelines

Module 7: Business Continuity Planning (BCP)

- Definition and Scope
- Components of a Contingency Plan
 - Disaster Recovery Plan
 - Emergency Mode Operation Plan
- Classification of Information
- Classification of Threats
- Types of Alternate Sites
- Getting Started
 - Conducting a Business Impact Analysis (BIA)
 - Key Activities
 - Developing Your Disaster Recovery Plan (DRP)
 - Critical Sections

Case Study: Conducting a Business Impact Analysis (BIA)

Step through key activities that organizations must conduct to complete a comprehensive Business Impact Analysis (BIA). Understand critical processes for a BIA initiative and identify areas that must be addressed in a BIA Report.

Module 8: Getting Compliant, Integrating Best Practices

- Information Security Strategy
- Enterprise Security Methodology
 - Critical Steps
 - Integrate Compliance Requirements
- Risk Analysis
 - Definition and Scope
 - Information System Activity Review
 - Key Project Phases
 - Vulnerability Assessment Tools
- NIST Security Guidelines
- Getting Started
 - Developing Your Information Security Policies

Case Study: Review Sample Information Security Policy Templates

Step through key sections of critical information security templates in-class. Review sample policy types and organization. All CSCS™ candidates that pass the exam will receive a complete set of information security policy templates free.

Use these templates to create or update your enterprise information security policies. Policies templates are influenced by the requirements for several regulations.

Recognition for Other Security Certifications Earned

This is an excellent program for professionals that have earned credentials such as CISSP, CISM, CISA, Security+, MCSE, and CBCP.

CISSP, CISM, CISA, Security+, MCSE and CBCP certified professionals will find that the CSCS™ program adds significant depth to their knowledge of compliance requirements related to information security. These compliance requirements directly impact the security priorities and initiatives across all types of organizations and business.

Exam Fee

The Certified Security Compliance Specialist™ (CSCS™) exam fee is \$495.00.

Requirements for Maintaining CSCS™ Certification

CSCSs must comply with the following requirements to retain certification:

- Comply with ecfirst.com Academy's Code of Professional Ethics.
- Re-certify once every three (3) years. Information on re-certification exams are announced at www.ecfirst.com/Academy. Re-certification exam fee is \$195.00.

Revocation of CSCS™ Certification

ecfirst.com Academy may, at its discretion after due and thorough consideration, revoke an individual's CSCS™ certification for any of the following reasons:

- Violating any provision of the ecfirst.com Code of Professional Ethics
- Falsifying or deliberately failing to provide relevant information
- Intentionally misstating a material fact
- Engaging or assisting others in dishonest, unauthorized or inappropriate behavior at any time in connection with the CSCS™ exam or the certification process

Training Options

The two-day Certified Security Compliance Specialist™ (CSCS™) program is delivered worldwide. Call the ecfirst.com Academy at **877.899.9974 x17** today to discuss details about locations and schedules.

CSCS™ program attendees may pursue additional career development with the Certified HIPAA Professional (CHP) program. Mention you have passed the CSCS™ exam and receive 20% off the instructor-led tuition fee for the CHP program.

On Site Training

Bring ecfirst.com Academy training, certification and executive briefs to your site. ecfirst.com Academy will customize the session to meet your specific requirements and time frames.

Reference Materials

ecfirst.com

ecfirst.com Academy is passionate about developing and validating information security compliance knowledge. ecfirst.com Academy, in business since 1999, was recognized as an Inc. 500 fastest growing privately held business in the United States in its first year of eligibility. ecfirst.com is an organization with deep hands-on experience in compliance and IT services.

ecfirst.com Academy is exclusively endorsed by the American Hospital Association (AHA) for its Training Solutions and is a partner of Illinois Hospital Association (IHA).



ecfirst.com serves a Who's Who client list that includes Wells Fargo, numerous hospitals including Edward, Sherman, Condell, BSA, Mercy, Northwest Community, Samaritan and many others. State and county governments that have been trained by ecfirst.com include the State of Oregon, Iowa, and Illinois. U.S. government agencies that have participated in ecfirst.com programs include the U.S. Department of Veterans Affairs, Air Force, Coast Guard, Homeland Security, Coast Guard and several others.

Disclaimer

This document is a guide to those pursuing the CSCS™ certification. No representations or warranties are made by ecfirst.com that the use of this guide or any other associate publication will assure candidates of passing the CSCS™ exam.

Disclosure

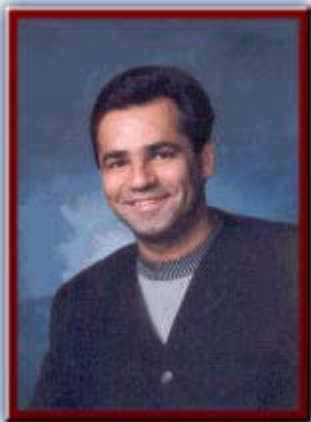
Copyright © 2006, 2007, 2008 by ecfirst.com. Reproduction or storage in any form for any purpose is not provided without prior written permission from ecfirst.com. No other right or permission is granted with respect to this work. All rights reserved.

Contact Information

14225 University Avenue, Suite 240
Waukee, Iowa 50263, United States
Phone: +1.515.453.8247 x17
Fax: +1.515.453.8471
Email: Lorna.Waggoner@ecfirst.com
Web-site: www.ecfirst.com

ecfirst.com Academy Program Architect

Uday **Ali** Pabrai, CISSP (ISSAP, ISSMP), CSCS, is the chief executive of ecfirst.com, an Inc. 500 business and an organization exclusively endorsed by the American Hospital Association (AHA). A highly sought after information security and regulatory compliance expert, he has successfully delivered solutions on healthcare information technologies to organizations across the United States.



Author of *PCI DSS Quick Reference Card*, he developed a unique security methodology called, BizShield: The Seven Steps to Enterprise Security. BizShield today provides the framework for many security initiatives at several client organizations.

He has delivered highly tailored security solutions to hundreds of clients across several industries.

Mr. Pabrai was the creator of the world's most successful Internet skills certification, CIW. Mr. Pabrai also established the industry's first certification program on HIPAA - Certified HIPAA Professional (CHP) and Certified HIPAA Security Specialist (CHSS). He recently launched the Certified Security Compliance Specialist (CSCS) program. Mr. Pabrai is the co-creator of the Security Certified Program (SCP) – a program approved by the U.S. Department of Defense Directive 8570.1M and one of the industry's most comprehensive hands-on information security certification program.

Mr. Pabrai has presented keynote and other sessions at several conferences, including ISSA, HCFA, HIPAA Summit, Internet World, DCI Expo, Comdex, Net Secure, Nurse Practitioners Conference, National Council for Prescription Drug Programs (NCPDP), National Council for State Board of Nursing IT Conference, and many others.

He has delivered fast paced, high energy briefings in many cities worldwide including New Delhi, Bangalore and Mumbai (India), Tsukuba City (Japan), Dubai (UAE), Karachi and Lahore (Pakistan), London (UK), and across the United States.

Mr. Pabrai's clients have included hundreds of hospitals, long term care facilities, Microsoft, Kemin, Intuit, Pella, Principal Financial, U.S. Naval Surface Warfare Center, U.S. Defense Intelligence Agency, U.S. Department of Veteran Affairs, as well as numerous federal, state and county governments.

His career was launched with the U.S. Department of Energy's nuclear research facility, Fermi National Accelerator Laboratory in Chicago. During his career, he has served as Vice Chairman and in several senior Officer Positions with NASDAQ-based firms.

Mr. Pabrai is a member of the U.S. FBI InfraGard.